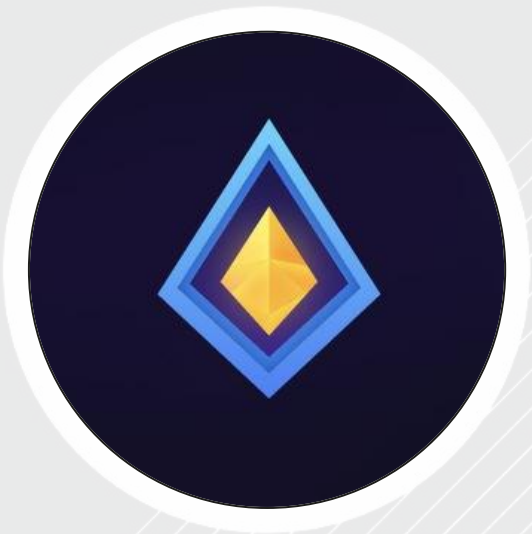
SPYWOLF

Security Audit Report



Completed on

December 13, 2023

OVERVIEW

This audit has been prepared for **STELLUM** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

STELLUM

PROJECT DESCRIPTION

According to their whitepaper:

“Stellum is a play to earn game that allows you to earn cryptocurrency while playing.

Explore space, discover new planets, hire workers to extract resources and most importantly - improve your NFT character.”

Release Date: Presale starts in December, 2023

Category: Play to earn (P2E)

CONTRACT INFO

Token Name
N/A

Symbol
N/A

Contract Address
0x309b15aAaBa64C4292E0825E8095C6BA6FD07CB3

Network
Base

Language
Solidity

Deployment Date
Dec 11, 2023

Contract Type
Staking

Total Supply
N/A

Status
Not launched

TAXES

Buy Tax
8%

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	N/A
Uniq Senders	N/A
Uniq Receivers	N/A
Total Amount	N/A
Median Transfer Amount	N/A
Average Transfer Amount	N/A
First transfer date	N/A
Last transfer date	N/A
Days token transferred	N/A

SMART CONTRACT STATS

Calls Count	9
External calls	9
Internal calls	0
Transactions count	9
Uniq Callers	4
Days contract called	2
Last transaction time	Dec-12-2023 05:55:23 PM +UTC
Created	Dec-11-2023 01:23:19 PM +UTC
Create TX	0x437ab543b3fa3340c741be6100f765e3719c74523fe1fad9bd5b3edab1d4a987
Creator	0x4e01af691fda86d5d4adc558a1f580e2642eee00

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can change uniswapRouter address.
If set to inappropriate address, investors might be unable to withdraw their rewards.

```
function changePancakeRouterAddress(address newAddr) external onlyOwner {
    require(newAddr != address(0x0) && Address.isContract(newAddr), "Invalid PancakeRouter address");
    require(newAddr != address(uniswapRouter), "Address is already setted");

    uniswapRouter = IUniswapV2Router02(newAddr);
}

function withdrawCrystals(uint256 crystalsAmount) external {
   ..............................
    address[] memory path = new address[](2);
    path[0] = address(token);
    path[1] = uniswapRouter.WETH();

    token.mint(address(this), crystalsAmount);
    token.increaseAllowance(address(uniswapRouter), crystalsAmount);

    uint256[] memory amounts = uniswapRouter.swapExactTokensForETH(
      crystalsAmount,
      0,
      path,
      msg.sender,
      block.timestamp + 5 minutes
    );
    uint256 ethAmount = amounts[1];

    player.withdrawn+= ethAmount;
..............................
}
```

- Recommendation:
  - uniswapRouter address should not be changed after initial deployment

FOUND THREATS

⚠ Medium Risk

Owner can change current coin address.
Coin address can be used to get advantage regarding upgrading the character, which can lead to higher yield.

```
function buyEnergy(address referrer) external payable {
.............
uint256 xp = msg.value * Constants.ENERGY_FOR_ETH * Constants.PERCENT_PRECISION / 1 ether;
player.xp+= xp * getXPMultiplier(msg.sender);
.............
}

function upgradeCharacter(uint8 toLevel, address coinAddress) external payable {
.....................
require(
    coinAddress == address(0x0) || coins[coinAddress].lpToken != address(0x0),
    "Invalid coin address"
);
.....................
uint256 coinsAmount;
if (upgradePriceETH > 0) {
    if (coinAddress == address(0x0)) {
    require(msg.value == upgradePriceETH, "Invalid upgrade ETH amount");

    payable(character.ETH_RECEIVER_ADDRESS()).transfer(msg.value);
    } else {
    require(msg.value == 0, "Invalid upgrade ETH amount");
    coinsAmount = getTokensAmount(coinAddress, upgradePriceETH);

    ICommonInterface(coinAddress)
        .transferFrom(msg.sender, character.ETH_RECEIVER_ADDRESS(), coinsAmount);
    }
}
.....................
}
```

```
function getXPMultiplier(address playerAddr)
 public view returns (uint256 xpMultiplier) {
    if (characters[playerAddr] == 0) {
      return Constants.PERCENT_PRECISION;
    }

    uint8 characterLvl = character.level(characters[playerAddr]);
    if (characterLvl >= 13) {
      return Constants.PERCENT_PRECISION + 30_00;
    } else if (characterLvl >= 11) {
      return Constants.PERCENT_PRECISION + 25_00;
    } else if (characterLvl >= 9) {
      return Constants.PERCENT_PRECISION + 20_00;
    } else if (characterLvl >= 7) {
      return Constants.PERCENT_PRECISION + 15_00;
    } else if (characterLvl >= 5) {
      return Constants.PERCENT_PRECISION + 10_00;
    } else if (characterLvl >= 3) {
      return Constants.PERCENT_PRECISION + 5_00;
    }

    return Constants.PERCENT_PRECISION;
}

function collectAchievementReward() external {
    GameModels.Player storage player = players[msg.sender];

    uint8 lvl = player.level + 1;
    while (lvl < ACHIEVEMENTS_NUMBER) {
      if (player.xp >= ACHIEVEMENTS_XP[lvl] * Constants.PERCENT_PRECISION
       * Constants.PERCENT_PRECISION) {
        balances[msg.sender].energy+= ACHIEVEMENTS_REWARDS[lvl];
        lvl++;
      } else {
        break;
      }
    }

    player.level = lvl - 1;

    emit Events.CollectAchievementReward(msg.sender,
     player.level, block.timestamp);
}
```

- Recommendation:
  - Coin address should not be changed

Informational

In total five contracts are involved in Stellum game as follows: Stellum main contract, NFT contract, Token contract, Uniswap router contract, Liquidity pair contract.

This audit is only for the Stellum main contrat.
Logic of the other involved contracts in game mechanics is **not** subject of this audit.

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

STELLUM

GOOD PRACTICES FOUND

This is **ROI** dapp. **ROI** dapps are usually subject to high volatility and considered as risk investments.

Game mechanics:
Players can buy energy with ETH. Energy is used to upgrade planets.
Players send rockets in space starting from 1 day per flight up to 10 days per flight to earn crystals and energy.
Players can buy character (NFT), which will increase their rockets flight duration time. Characters must be attached to the Stellum main contract in order to receive bonuses from them.
Players can upgrade their character up to 20 times and on each upgrade they will receive more crystals per day productivity.
Players can exchange their crystals for STM token and exchange the STM token to ETH.
There are 8 planets available for users to upgrade with max 50 updates for each planet.
Users can proceed to next level planet once they reach at least 30 updates on the previous planet.

Players can have up to 7 referrals and up to 12% earned in energy and ETH.
On each energy buy, players can specify their referral address.
If referral address is chosen to be address(0) or depositor itself, referral becomes the default referral set by the contract owner.
If referral address does not participate in the game yet, referral becomes the default referral set by the contract owner

**ROI - Return of investment*

TOKENOMICS

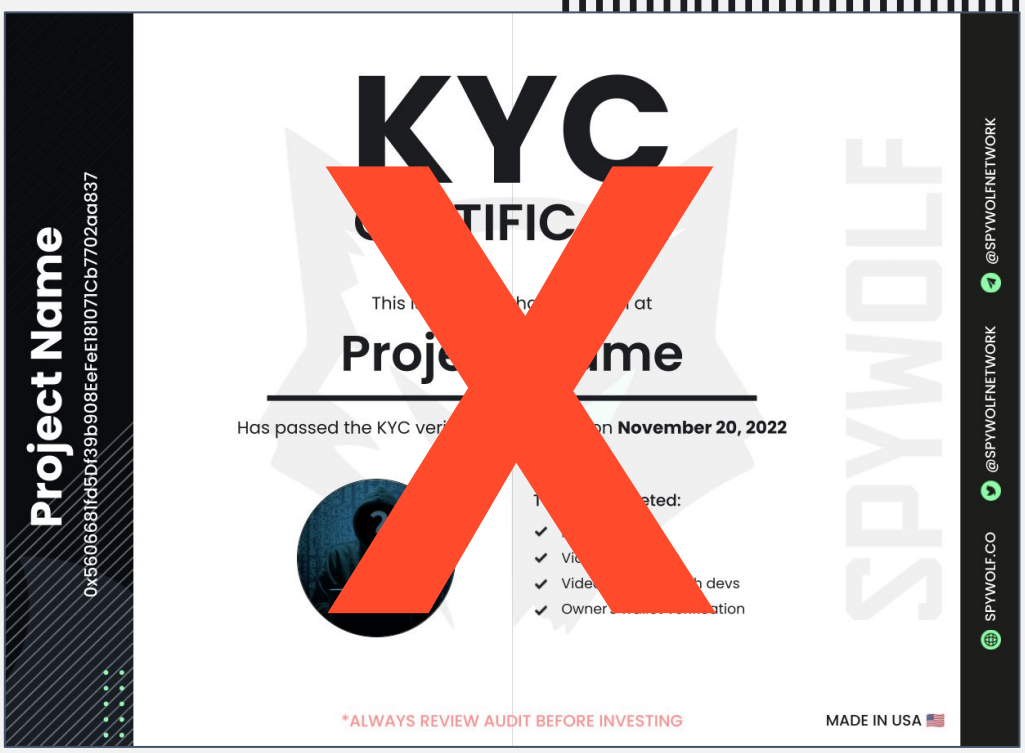
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://stellum.io/

Domain Registry
https://www.namecheap.com/

Domain Expiration
2024-10-19

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

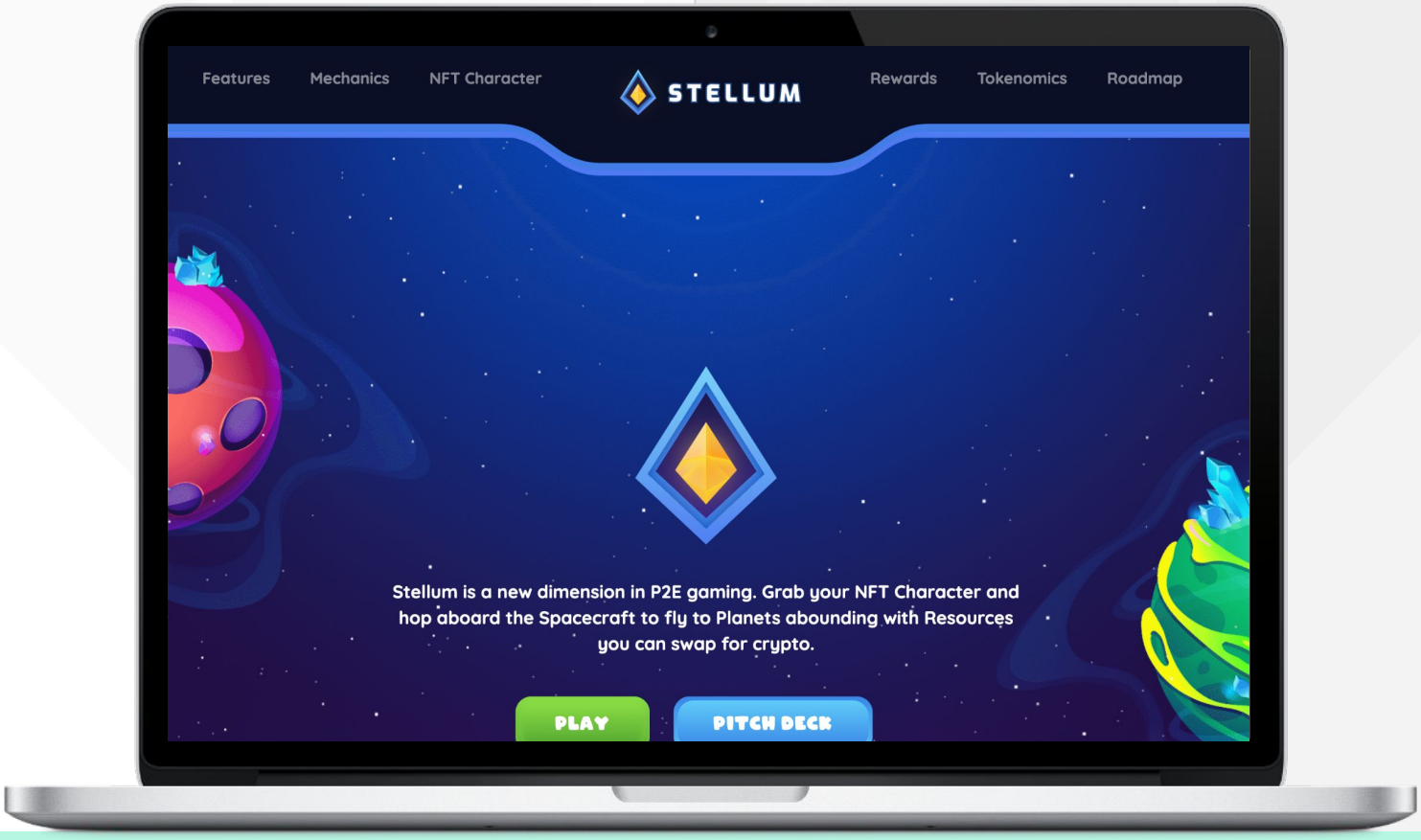
Design
Very nice overall design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found..

Whitepaper
Yes, explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



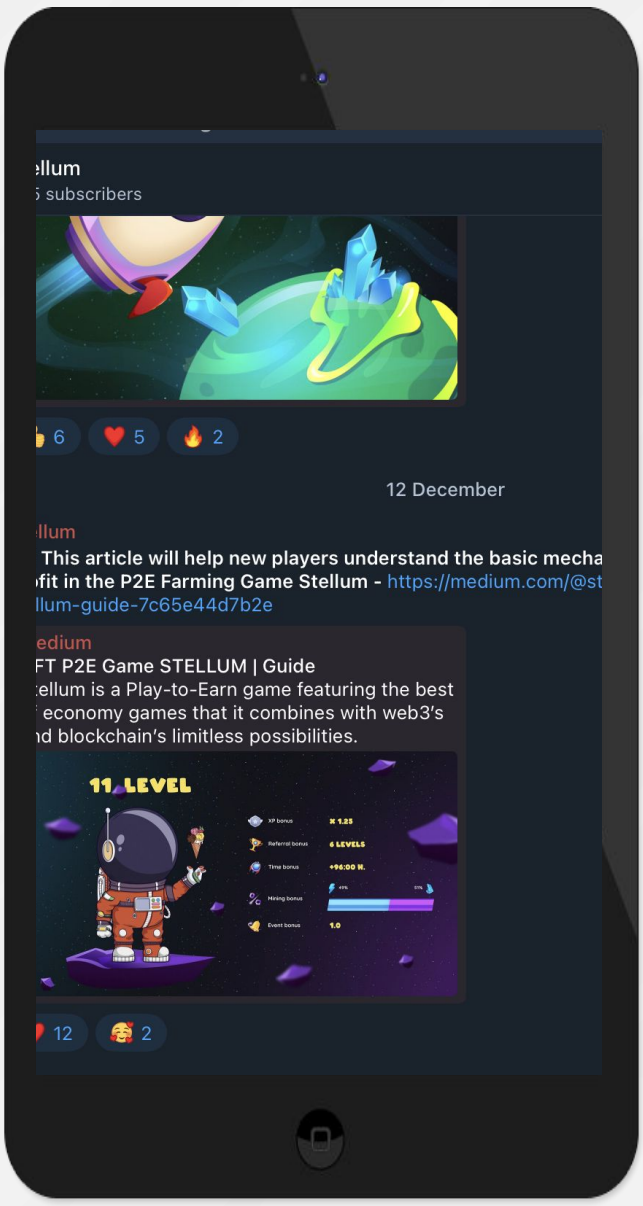
stellum.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter

@stellum_io

- Account suspended!

Telegram

@stellum_group

- 6 881 members
- Active members
- Active mods

Telegram

@stellum

- 409 subscribers
- Announcement channel
- Dormant from february with renewed activity since November

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.